

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

Rules and Regulations Implementing the)	
Telephone Consumer Protection Act of 1991)	CG Docket No. 02-278
)	
Establishing Just and Reasonable Rates for)	
Local Exchange Carriers)	WC Docket No. 07-135

COMMENTS OF VERIZON

Kathleen Grillo
Of Counsel

John T. Scott, III
Christopher D. Oatway
1300 I Street N.W., Suite 400 West
Washington, D.C. 20005
(202) 515-2470

Attorneys for Verizon

January 23, 2015

TABLE OF CONTENTS

	SUMMARY	1
I.	INDUSTRY IS FIGHTING THE ROBOCALL PROBLEM ON MULTIPLE FRONTS.....	2
A.	Efforts Are Underway to Help Stop Illegal Robocalls at Their Source	3
B.	Existing Tools Empower Consumers to Stop Unwanted Robocalls from Ringing on their Phones	5
II.	STRENGTHENING EXISTING ANTI-ROBOCALL MEASURES.....	7
A.	Government Can Help By Increasing Consumer Education And Awareness of How to Stop Robocalls.....	7
B.	Better Laws and Better Enforcement Can Help Stop More Robocalls at the Source	8
III.	ALL STAKEHOLDERS NEED TO DRIVE TOWARD TECHNOLOGY THAT WILL MAKE REAL-TIME BLOCKING OF ROBOCALLS SUSTAINABLE ON A LARGE-SCALE BASIS	8
A.	Network-Based Blocking Currently Faces Substantial Technological Challenges	8
B.	Promising New Solutions to Address Robocalls Are Under Development	9
	CONCLUSION	11

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

Rules and Regulations Implementing the)	CG Docket No. 02-278
Telephone Consumer Protection Act of 1991)	
)	
Establishing Just and Reasonable Rates for)	WC Docket No. 07-135
Local Exchange Carriers)	

COMMENTS OF VERIZON¹

SUMMARY

Verizon agrees with the National Association of Attorneys General (NAAG)² and the Commission³ that widespread illegal robocalls are a problem that needs to be addressed on many fronts. This is an issue on which the industry and policymakers have a common interest, in order both to protect customers and to address the significant costs imposed by robocall schemes.

Verizon and other carriers employ today a variety of measures to stop millions of illegal robocalls at their source, before they can ring on anyone's phone. In addition, consumers also have a variety of tools available to them to directly manage what calls do or do not ring on their phones. There is no "one-size-fits all" solution to the problem of widespread illegal robocalls.

Part of the solution can and must be more effective consumer education efforts to empower

¹ In addition to Verizon Wireless, the Verizon companies participating in this filing are the regulated, wholly owned subsidiaries of Verizon Communications Inc. (collectively "Verizon").

² See Letter from National Assoc Attys General, dated Sept. 9, 2014, to FCC Chairman Tom Wheeler, CG Docket No. 02-278 & WC Docket No. 07-135 (Nov. 20, 2014) ("*NAAG Letter*").

³ See Public Notice, *Consumer And Governmental Affairs Bureau Seeks Comment On Robocalls and Call-Blocking Issues Raised by The National Association of Attorneys General on Behalf Of Thirty-Nine Attorneys General*, CG Docket No. 02-278 & WC Docket No. 07-135; DA 14-700 (Nov. 24, 2014) ("*Notice*").

consumers to protect themselves, along with an “all of the above” strategy under which all stakeholders utilize and strengthen existing mitigation techniques, while redoubling efforts that are underway to develop longer-term IP-based solutions to the robocalling problem.

DISCUSSION

I. INDUSTRY IS FIGHTING THE ROBOCALL PROBLEM ON MULTIPLE FRONTS.

The industry and policy makers have a common interest in combatting illegal robocalls. Robocalls, which are often (but not always) illegal, particularly affect landline customers, who are often targeted by unscrupulous telemarketers and fraudsters, and whose protections under the Telephone Consumer Protection Act (TCPA) are less than those that wireless customers enjoy.⁴ But carriers’ fraud and customer care teams also field robocall complaints from wireless customers, such as recent “one-ring” scams aimed at inducing customers to inadvertently dial international numbers.⁵ Moreover, robocalls affect the availability of both wireline and wireless networks because mass calling events can overwhelm switches and prevent legitimate calls from completing. In addition to being a burden on our customers, robocalls impose significant costs on companies like Verizon. Addressing these problems requires significant time and resources from customer care and fraud teams, which address complaints about abusive telemarketing and other scams perpetrated by robocallers, and network engineers who monitor the network for suspicious calling, take steps to prevent robocalls, and provide support to law enforcement and

⁴ For example, the TCPA prohibits all non-emergency robocalls to wireless customers without their consent, but does not prohibit autodialed or prerecorded calls to residential customers from tax-exempt nonprofit organizations. *Compare* 47 U.S.C. § 227(b)(1)(A)(iii) *with* 47 U.S.C. § 227(b)(1)(B) and 47 U.S.C. § 227(b)(2)(B).

⁵ *See, e.g.*, “‘One Ring’ Phone Scam,” <http://www.fcc.gov/guides/one-ring-wireless-phone-scam>.

other government agencies in their efforts to track down and shut down illegal robocallers. Accordingly, as discussed below, Verizon is committed to fighting robocalls on various fronts.

A. Efforts Are Underway to Help Stop Illegal Robocalls at Their Source.

While millions of robocalls traverse the nation's PSTN every month, they are needles in a haystack compared to the tens of billions of local, long distance and international calls that Verizon delivers every month. The fact that robocalls normally arrive via multiple routes, as opposed to coming from a single telephone number (or even from a single NPA-NXX), also makes it challenging to identify suspicious calling patterns in real time. Adding to that challenge is the fact that the calling patterns of illegal robocalls often mimic legitimate robocalls (e.g., school closings, airline cancellations). Verizon's engineers have responded by using "honeypots" that collect information about traffic flows in our network. They do not monitor call content but rather are tools for proactive analysis of robocalling trends. Verizon's engineers combine that data collection with data analytics to identify suspicious calling patterns based on call volumes, call routing, call destinations, and call durations and completion rates.

Verizon's network engineers and fraud experts use those data analytics to address the robocall problem. When Verizon detects a suspicious pattern of calls that arrives on Verizon's network through an interconnection point with another carrier, Verizon will coordinate with the carrier(s) in the call path to identify the originating carrier, and will request that the originating carrier investigate its robocall customer so that the customer can discontinue service if it determines its customer is breaking the law. Such efforts to trace back and shut down suspected illegal robocall activity are common throughout the industry when there is a suspicious pattern of robocalls. Similarly, when a suspicious traffic pattern arrives on Verizon's network via one of Verizon's wholesale customers, Verizon contacts the wholesale customer to request that the

wholesale customer immediately investigate such traffic and ascertain whether the traffic is legitimate and, if not, to cease transmitting such traffic to Verizon.⁶

Also, Verizon's TCPA experts and its fraud teams work closely with various law enforcement agencies, supporting their efforts to investigate and prosecute illegal robocall scams. They routinely help enforcers trace the source of suspicious calls by promptly responding to duly served subpoenas. In addition, Verizon's network engineers have, under similar circumstances, helped enforcers demonstrate that suspicious calls were generated from autodialers by analyzing the calling patterns and providing appropriate expert affidavits. Verizon also brings TCPA lawsuits against robocallers to protect its customers from illegal robocalls. For example, as a TCPA plaintiff, Verizon recently secured a federal court order that shut down a robocall scam in which millions of customers received calls asking them to provide personal information in exchange for the promise of a "free cruise."⁷

These efforts to track down and shut down illegal robocallers constitute the largely-unseen "front lines" of the fight against robocalls. Consumers would be inundated with even more robocalls if Verizon and other carriers did not undertake these sustained day-to-day efforts to keep such illegal robocalls off their networks.

⁶ To the extent Verizon were to learn of suspicious traffic patterns generated by a Verizon retail customer, we would similarly pursue appropriate remedies as permitted by law and by applicable contracts and tariffs.

⁷ See Consent Order Granting Permanent Injunctive Relief, *Cellco Partnership d/b/a/ Verizon Wireless v. Plaza Resorts, Inc.*, Case No. 9:12-CV-81238-KAM (S.D. Fla. issued Sept. 15, 2014).

B. Existing Tools Empower Consumers to Stop Unwanted Robocalls from Ringing on their Phones.

In addition to stopping illegal robocalls at their source, Verizon offers wireline and wireless customers various tools they can use to stop receiving them. Apart from tools like Anonymous Call Rejection which permit customers to manage what calls ring on their phones, Verizon (and other carriers) offer Caller ID, a service customers can use to filter calls visually (answering only if they recognize the caller's number) or to take advantage of tools that manage the calls that ring on their phones. Customers can also use various third-party solutions that leverage the Caller ID functionality to permit customers to tailor the calls they receive to their specific preferences.

Wireless customers can download a variety of apps that use the Caller ID functionality to reject or screen calls from telephone numbers that the apps identify as suspicious based on various techniques such as crowd-sourcing algorithms or blacklists of complained-of numbers.⁸ They can also take advantage of their smartphones' built-in features which permit them to manage which calls will ring on their phones and which will not. On the wireline side, customer premises equipment (CPE) manufacturers offer blacklist/whitelist based call rejection solutions as well as other tools to filter out robocalls, such as CAPTCHA⁹ devices that pass certain calls through menus designed to weed out non-human callers.¹⁰ Some of these third-party solutions

⁸ See, e.g., Herb Weisbaum, "Want to get rid of those \$#%@ robocalls? There's an app for that," available at <http://www.cnbc.com/id/101758815#>.

⁹ CAPTCHA is the acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart."

¹⁰ See, e.g., T-Lock Call Blocker – Version N2, http://hqtelecom.com/callblocker?gclid=CMmt_raT6cECFc1_MgodhnEAWg; CPR Call Blocker Product Page, <http://www.cprcallblocker.com/purchase.html>; Digitone Call Blocker Plus, <http://www.digitone.com>; Sentry Dual Mode Call Blocker,

also give consumers the option to reject – at each individual consumer’s direction and with no carrier involvement – particular types of calls, such as political robocalls, that some consumers may not want but that Congress has deemed to constitute legitimate traffic.

The Federal Trade Commission (FTC) has highlighted the diversity of third party solutions that consumers can use on a variety of platforms to protect themselves from robocalls. For example, one of the practical suggestions that the FTC received in response to the “consumer tip” portion of the FTC Robocall Challenge was that consumers can consider exploring the devices available to block calls to landline phones.¹¹ Another tip that the FTC passes on to consumers is to investigate apps for their smartphones.¹²

None of these end user-directed solutions is a panacea, and currently bad actors can find ways to bypass any particular approach. Also, these solutions can potentially have harmful unintended consequences. For example, anti-robocall smartphone apps and CPE may prevent consumers from receiving wanted calls if they rely on blacklists that inadvertently include numbers of legitimate callers – which can happen for a variety of reasons, including if fraudulent robocallers have spoofed legitimate customers’ numbers, thereby causing them to be blacklisted. Indeed, widespread deployment of blacklist-based products could lead to more spoofing than already occurs because robocallers would have increased incentives to bypass the protections those products provide. But on balance consumers are likely to benefit from the ability to choose from a diverse array of products that use different techniques to mitigate (by filtering, rejecting,

<http://www.plugnblock.com/?gclid=CJmKkbaT6cECFSFgMgodJRIAGA>; and Privacy Corp Caller ID Manager, <http://www.privacycorps.com/products/>.

¹¹ See Tip No. 2, “Tips and Tricks” video, *available at* <http://www.consumer.ftc.gov/media/video-0086-robocall-challenge-consumer-tips-tricks> (last visited Jan. 23, 2015).

¹² *Id.*, Tip No. 4.

blocking, or simply warning consumers about) calls – whether legal or illegal – that the consumers may not want.

II. STRENGTHENING EXISTING ANTI-ROBOCALL MEASURES.

A. Government Can Help By Increasing Consumer Education And Awareness of How to Stop Robocalls.

Dedicating more government resources to educating consumers about robocalls would go a long way toward ensuring consumers know what they should and should not do when they receive unwanted calls, and making them aware of the various options they have to protect themselves from such calls. Although the existence of the Do Not Call List has been widely publicized, some consumers remain confused about what sorts of call are permitted to telephone numbers on the list. Some consumers therefore complain about calls that are legal, such as ones from nonprofit organizations to residential lines. And many consumers still may not realize that it is inadvisable to call back the robocaller (or to press a number to purportedly be “taken off the list”) because doing so is likely to cause robocallers to target the consumer even more aggressively. The FTC today provides advice to consumers on its web site, much of which could be marshalled by other stakeholders to ensure that consumers are well informed about what they should and should not do.¹³

Also, many consumers may be unaware of the products available to them to manage the types of calls they receive. As mentioned above, the FTC has flagged the availability of third-party devices for wireline customers, but all stakeholders can take steps to ensure that consumers understand the various options available to them. At the same time, it is important to recognize

¹³ See, e.g., “What to Do if You Get a Robocall” video, *available at* <http://www.consumer.ftc.gov/media/video-0028-what-do-if-you-get-robocall> (last visited Jan. 23, 2015).

that those products will vary in their effectiveness, and that some may raise policy issues. For example, overbroad blacklists could harm innocent non-subscribing customers, who may find themselves blacklisted through no fault of their own. And some third parties may offer products that raise privacy issues, including if they collect information about their users or if they examine the contents of any calls. Therefore, an important component of consumer outreach should be to ensure that consumers are not only aware of the third party robocall mitigation options available to them, but also to help evaluate the pros and cons of those options.

B. Better Laws and Better Enforcement Can Help Stop More Robocalls at the Source.

As discussed above, Verizon's attorneys and fraud teams are engaged in efforts to shut down robocalls operations that violate the TCPA, including by bringing private lawsuits and by assisting law enforcement officials with investigating and prosecuting such scams. The Commission should encourage and facilitate strong TCPA enforcement through improved cooperation between industry and state and federal law enforcement agencies. Also, all stakeholders should work to explore ways to improve existing laws to more effectively target robocallers that annoy, harass, or defraud consumers.

III. ALL STAKEHOLDERS NEED TO DRIVE TOWARD TECHNOLOGY THAT WILL MAKE REAL-TIME BLOCKING OF ROBOCALLS SUSTAINABLE ON A LARGE-SCALE BASIS.

A. Network-Based Blocking Currently Faces Substantial Technological Challenges.

Barriers to entry are very low for robocallers, who can use computers with Internet connections to blast consumers with massive numbers of calls while employing techniques, including Caller ID spoofing, to avoid detection and to bypass mitigation efforts. Although Verizon has a sophisticated data analytics program that we use to identify suspicious calling

patterns, we cannot unambiguously identify illegal robocalls on a real-time basis as they cross our network. That is because carriers only have visibility into robocalls once they reach our networks; because illegal robocalls can travel via a diversity of routes and can mimic legitimate traffic (such as school closings, airline cancellations, or bad weather alerts); and because any solution that relies on a blacklist of unwanted numbers can be bypassed by robocallers who spoof legitimate numbers. Indeed, any large-scale deployment of a blacklist-based blocking solution would risk increasing the amount of “spoofing” that already occurs.

Although Verizon would not object to clarification of any exceptions to the Commission’s ruling that carriers may not “block, choke, reduce or restrict traffic in any way,”¹⁴ these current technological challenges would make it impractical to effectively block robocalls as they traverse the PSTN. The Commission’s existing policies are not impeding the work Verizon and others are already doing to take millions of robocalls off the PSTN by shutting down illegal robocall operations, nor are they constraining consumers’ ability to use existing robocall mitigation products to directly protect themselves from unwanted robocalls. And they are not slowing the work of Verizon and others to develop new technologies that hold promise for an eventual blocking solution that can be deployed on a sustainable and large-scale basis.

B. Promising New Solutions to Address Robocalls Are Under Development.

Verizon participates in various industry fora that are developing enhanced techniques for combatting robocalls. One is the Voice and Telephony Abuse Special Interest Group (VTA-SIG) of the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG). The VTA-SIG has recently been focusing on developing improved honeypot programs and data

¹⁴ See *Establishing Just and Reasonable Rates for Local Exchange Carriers*, Declaratory Ruling and Order, 22 FCC Rcd 11629, ¶ 6 (2007).

analytics as well as improved reporting and sharing of robocall information among various stakeholders. Working groups have been created within M³AAWG to update and republish “Best Practices to Address Online and Mobile Threats,” with Verizon providing resources for the “Telephony: Mobile and Instant Messaging Threats, VoIP and Caller ID Abuse” working group.¹⁵

Verizon also participates in many of the committees within the Alliance for Telecommunications Industry Solutions (ATIS) to develop relevant standards and solutions for the industry. Verizon’s ATIS involvement includes a leadership role in the Next Generation Interconnection Interoperability Forum (NGIIF), which focuses on next generation technologies and recently published an “Auto Dialers Reference Document” that shares with other industry participants some of the key learning on robocallers, their methods, and mitigation techniques.¹⁶

Verizon and others are also addressing the challenges presented by Caller ID spoofing. No whitelist or blacklist solution will be sustainable on a large-scale basis unless there is a protocol with which a caller’s identity can be authenticated on a real-time basis. Development of such a protocol is one of the principal projects of the Internet Engineering Task Force (IETF), in which Verizon has been participating, and it has been the subject of substantial intellectual property development by Verizon engineers. The tools being developed by Verizon and its partners in these organizations will strengthen the protections available to stop illegal robocalls.

¹⁵ *Best Practices to Address Online and Mobile Threats*, http://cauce.typepad.com/files/best_practices_to_address_online_and_mobile_threats_oct_2012-2.pdf.

¹⁶ See Alliance for Telecommunications Industry Solutions, *Next Generation Interconnection Interoperability Forum (NGIIF) Auto Dialers Reference Document*, available at <https://www.atis.org/docstore/product.aspx?id=26137> (last visited Jan. 23, 2015).

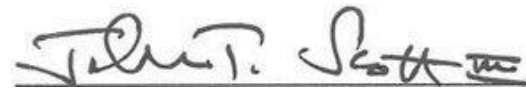
Given the limitations inherent in POTS networks, we expect that these next-generation robocall mitigation tools will be more robust once industry has made the transition to IP-based networks.

CONCLUSION

The Commission and other stakeholders should embrace an “all of the above” approach to robocall mitigation that stops illegal robocalls at the source, empowers consumers to stop annoying and unwanted robocalls at their home or handset, and drives towards eventual IP-based tools for identifying and mitigating robocalls.

Respectfully submitted,

Of Counsel:
Kathleen Grillo

A handwritten signature in dark ink, appearing to read "John T. Scott, III", written over a horizontal line.

John T. Scott, III
Christopher D. Oatway
1300 I Street N.W., Suite 400 West
Washington, D.C. 20005
(202) 515-2470

Attorneys for Verizon

January 23, 2015